Guidelines for Writing Cryptography Specifications

draft-irtf-cfrg-cryptography-specification-00
IETF 117, San Francisco
Writing cryptography specifications is a complex process that requires both technical knowledge and creative problem-solving. This document intends to give authors a comprehensive set of guidelines for creating a useful cryptography specification.
Goals, Requirements for Specification Authors

Minimize ambiguity and misinterpretations
- Leading to clearer specifications and more accurate implementations

Ensure consistent and correct implementation
- Providing precise instructions and explanations

Facilitate review and analysis
- Allowing for the verification of security properties and the identification of potential vulnerabilities

Enable standardization and interoperability
- Promoting collaboration and compatibility between various systems and protocols

By following these guidelines, specification authors can create documents that facilitate the development, analysis, and implementation of cryptographic solutions.
Call for Adoption Feedback

- References to previous RFCs
  Suggestions to more fully reference and utilize previous RFCs such as RFC 1700 (bits and bytes), RFC 5234 (ABNF), and RFC 8259 (JSON).

- Use of Standard Mathematical Symbols
  Some questions around the notation for specific operations like group operations, XOR, exponentiation.

- Question of ASCII vs Unicode
  Should recommendations explicitly define symbols using ASCII only?

- Clarity on terminology
  Terms like "formality" should be better defined as different audiences have different understandings.

- Broad support and review commitments
  Wide support for adoption with promises of full reviews with feedback.

- Specific focus on parameter choice
  Suggestion that parameter choice and security level should be discussed in all drafts.
Guidelines for Writing Cryptography Specifications

draft-irtf-cfrg-cryptography-specification-00
IETF 117, San Francisco